Add-On Products And Plug-Ins

This section contains information on the protection of various Natural add-on products by Natural Security and the handling of plug-ins in a Natural Security environment. It contains information on:

- Plug-Ins under Natural Security
- SYSDIC under Natural Security
- SYSAOS under Natural Security

Plug-Ins under Natural Security

The Natural Studio user interface is extensible by so-called "plug-ins". If plug-ins are used in an environment protected by Natural Security, the following prerequisites must be met:

Library Profiles for System Libraries

For the Natural plug-in manager (which is a plug-in itself) and for every plug-in to be used, a library security profile has to be defined. For plug-ins delivered together with Natural, pre-defined system-library profiles are provided. To activate these, you use the Administrator Services function "Definition of system libraries".

The following plug-in system libraries are provided:

Library	Contents
SYSPLMAN	The plug-in for the plug-in manager.
SYSEXPLG	A sample plug-in.
SYSPLXRC	The plug-in for the cross-reference GUI client.

User Profiles

When a user invokes a plug-in, the Natural plug-in manager starts a second Natural session with automatic logon (profile parameter AUTO=ON). For the automatic logon to be successful, a user who is to use a plug-in must have either a default library or a private library specified in his/her security profile.

Natural Parameter File

When a user invokes a plug-in, the Natural plug-in manager starts a second Natural session using the parameter file NATPARM. If the user’s Natural session uses a parameter file other than NATPARM, the system-file specifications for FNAT, FSEC and FUSER in the NATPARM parameter file must match those of the parameter file used by the user session in a Natural Security environment.

SYSDIC under Natural Security

On mainframe computers, the Predict library SYSDIC (which is described in the Predict documentation) may also be defined and its use controlled by Natural Security.

In the security profile of the library SYSDIC, the user exit NSCPRD01 must be specified. This user exit is entered into the security profile by executing the program NSCPRDAX in the library SYSSEC; the user exit is written into the security profile and *cannot* be overwritten there. The program must be executed to write the user exit into the security profile, otherwise you will not be able to use under Natural Security those Predict functions which use Adabas Online Services (AOS) facilities. (To delete NSCPRD01 from the security profile of SYSDIC, the program NSCPRDDX may be executed in library SYSSEC.)

After the user exit NSCPRD01 has been written into the security profile, no Predict functions will be available until Predict security profiles are defined.

You have to perform the following steps:

1. Create a security profile for the library SYSDIC (Add Library).
2. Execute program NSCPRDAX.
3. Iinvoke the Modify Library function for the library SYSDIC.

Even if you do not modify anything in the security profile of SYSDIC, you must perform this third step so as to confirm the entry of the user exit, because otherwise Natural Security will consider the execution of NSCPRDAX an illegal manipulation of SYSDIC’s security profile and no-one will be able to log on to SYSDIC. (The same applies if NSCPRDDX is executed.)

The library SYSDIC must be defined as people-protected.

When you select "User Exit" from the Additional Options of SYSDIC’s Library Profile, an additional screen "Predict/AOS Security Profile" will be displayed; on this screen you may specify who is to be AOS security administrator for which database. For each database you can only specify one AOS security administrator; this may be a user of type ADMINISTRATOR, PERSON, MEMBER, or a GROUP (it need not be a Natural Security administrator). The user must be linked to the library SYSDIC before he/she can be specified as AOS security administrator. The user (or group of users) specified may use the AOS-related Predict functions for the corresponding database.

For further information on Predict and its AOS-related functions, and on Predict under Natural Security, please refer to the Predict documentation.

SYSAOS under Natural Security

On mainframe computers, the Adabas Online Services library SYSAOS (which is described in the Adabas documentation) may also be defined and its use controlled by Natural Security.

The library SYSAOS must be defined as people-protected.

In the security profile of the library SYSAOS, the user exit NSCAOSE1 must be specified. This user exit is entered into the security profile by executing the program NSCAOSAX in the library SYSSEC; the user exit is written into the security profile and *cannot* be overwritten there. The program must be executed to write the user exit into the security profile, otherwise you will not be able to use the Security Maintenance section of Adabas Online Services under Natural Security. (To delete NSCAOS01 from the security profile of SYSAOS, the program NSCAOSDX may be executed in the library SYSSEC.)

After the user exit NSCAOS01 has been written into the security profile, no Adabas Online Services functions will be available until Adabas Online Services security profiles are defined.

You have to perform the following steps:

1. Create a security profile for the library SYSAOS (Add Library).
2. Execute program NSCAOSAX.
3. Invoke the Modify Library function for the library SYSAOS.

Even if you do not modify anything in the security profile of SYSAOS, you must perform this third step so as to confirm the entry of the user exit, because otherwise Natural Security will consider the execution of NSCAOSAX an illegal manipulation of SYSAOS’s security profile and no-one will be able to log on to SYSAOS. The same applies if NSCAOSDX is executed.

When you select "User Exit" from the Additional Options of SYSAOS’s Library Profile, an additional screen "Adabas Online Services Security Profile" will be displayed; on this screen you may specify who is to be Adabas Online Services security administrator for which database. For each database you can only specify one Adabas Online Services security administrator; this may be a user of type ADMINISTRATOR, PERSON, MEMBER, or a GROUP (it need not be a Natural Security administrator). The user must be linked to the library SYSAOS before he/she can be specified as Adabas Online Services security administrator. The user (or group of users) specified may use the Security Maintenance section of Adabas Online Services for the corresponding database.

For further information on Adabas Online Services, please refer to the Adabas documentation.

